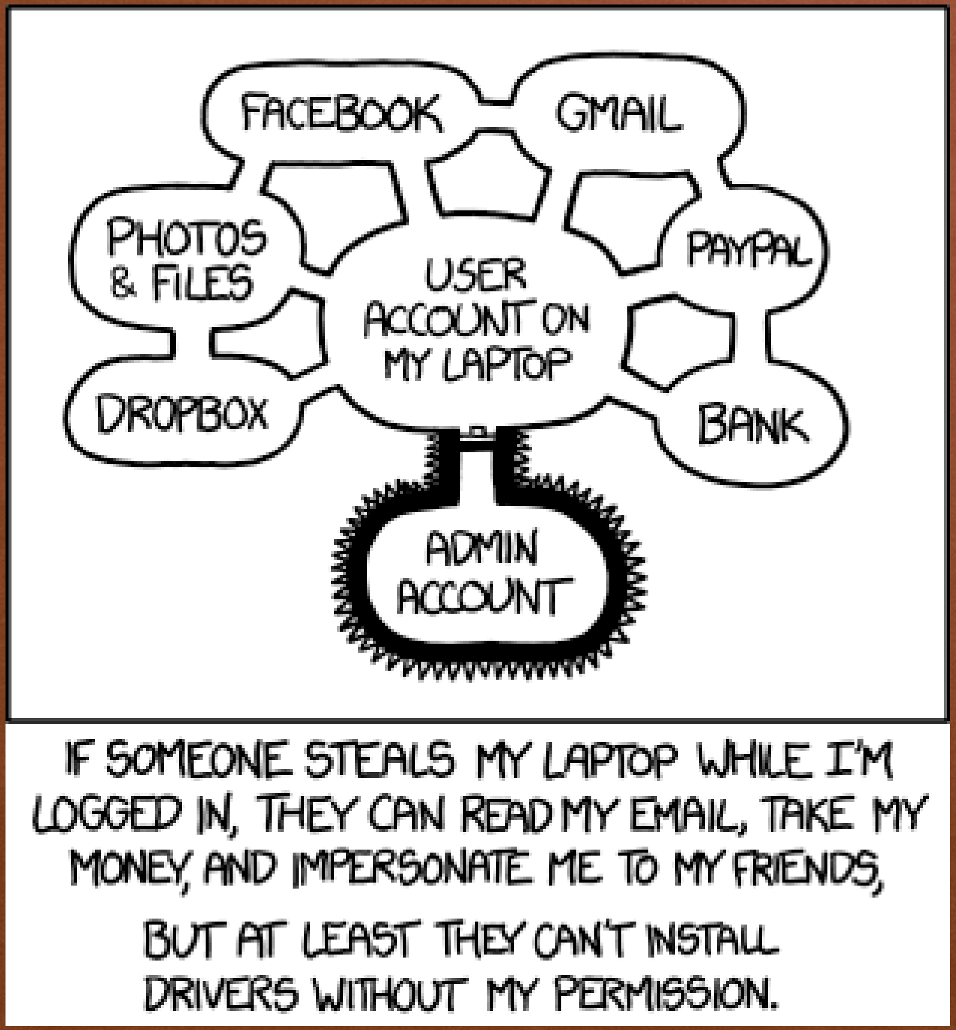
SECURITY

Chapter 8



https://xkcd.com/1200/

ASSYMMETRIC ENCRYPTION
(or PUBLIC-KEY ENCRYPTION)

Diffie-Hellman Example

Agreed upon numbers : p = 23 (modulus), g = 5 (base)

Alice’s secret a = 6

Public key (A) →
5^6 mod 23 = 8

Shared secret →
19^6 mod 23 = 2

Bob’s secret b = 15

Public key (B) →
5^15 mod 23 = 19

Shared secret →
8^15 mod 23 = 2

ASSYMMETRIC ENCRYPTION (or PUBLIC-KEY ENCRYPTION)

RSA key exchange

Let **P** : plain text, **C** : cipher text,
e : encryption key , **d**: decryption key.

P and C are digital values. We can think of the encryption and decryption processes as being inverse of each other.

Encrypt : $P^e \bmod n = C$

Decrypt : $C^d \bmod n = P$

ASSYMMETRIC ENCRYPTION (or PUBLIC-KEY ENCRYPTION)

RSA key exchange

Public key = (n, e)   Private Key = d

Here, $n = p*q$; *where* p *&* q *are two very large prime numbers*

In practice, n is as large as 2048 or 4096 bits

Though n is part of the public key, it is computationally difficulty to find two prime factors of n in finite time. This is strength of RSA.

ASSYMMETRIC ENCRYPTION (or PUBLIC-KEY ENCRYPTION)

RSA key exchange - steps

1. Pick 2 large prime numbers: p and q

2. Compute $n = p \times q$, and $m = (p - 1) \times (q - 1)$

3.Choose a number e at random so that e is co-prime with m and n (no common factors except 1) - Number **e** must be greater than 1 and less than m.

4.This guarantees that there will be some number d, between 0 and m, such that $(e \times d) \bmod m = 1$
(or equivalently $e \times d \cong 1 \bmod m$)

Public key = (n, e); Private key = d

ASSYMMETRIC ENCRYPTION (or PUBLIC-KEY ENCRYPTION)

RSA key exchange - example

1. $p = 7$, $q = 13$
2. $n = 7 \times 13 = 91$, $m = 6 \times 12 = 72$
3. Let $e = 5$ $(5 = 5 * 1)$
4. $e*d \bmod 72 = 1 \rightarrow 5*d \cong 1 \bmod 72 \rightarrow d=29$

Public key = (91, 5); Private key = 29

ASSYMMETRIC ENCRYPTION (or PUBLIC-KEY ENCRYPTION)

RSA key exchange - example

For the previous example, let's say message P = 37 (text mapped from char to numbers somehow)

Public key = (91, 5); Private key = 29

RSA encryption

Calculate $C = P^e \bmod n$

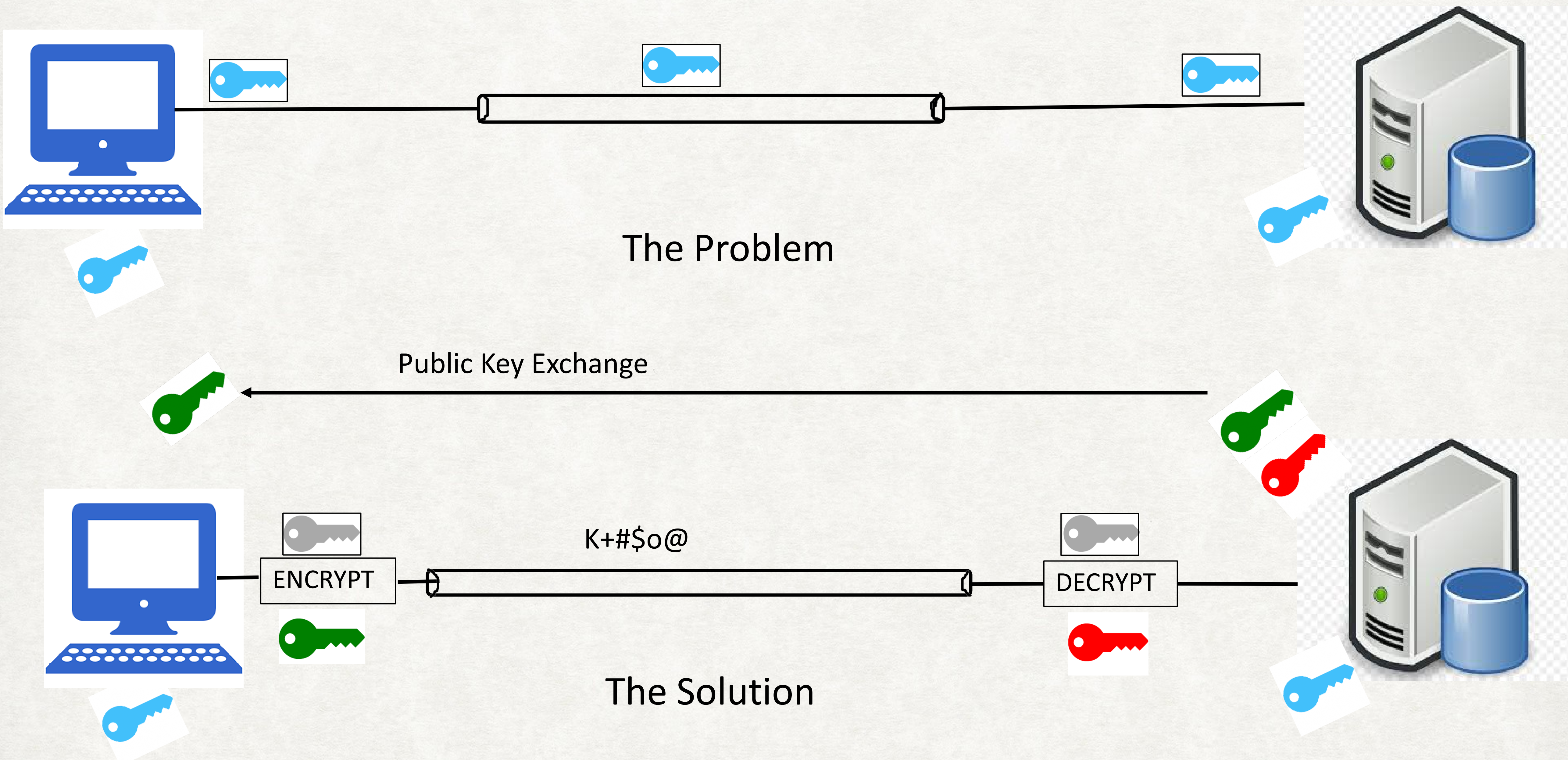
Calculate $C = 37^5 \bmod 91 = 46$

RSA decryption

Calculate $C^d \bmod n = P$

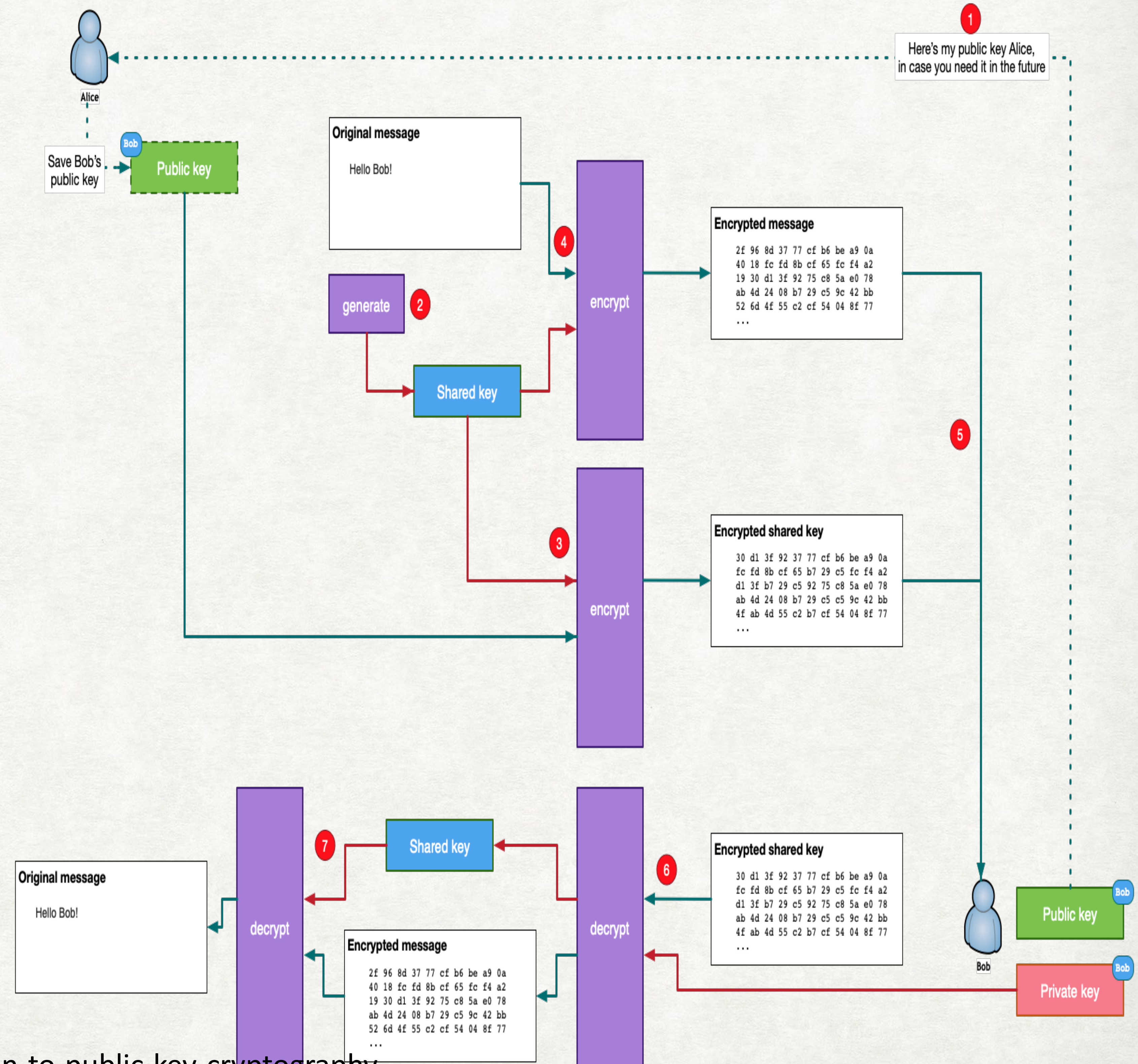
Calculate $46^{29} \bmod 91 = 37$

REVISITING - SECRET KEY DISTRIBUTION



REVISITING - SECRET KEY DISTRIBUTION

1. Bob sends his public key to Alice.
2. Alice generates a shared symmetric key.
3. Alice encrypts the symmetric key with Bob's public key.
4. Alice encrypts the message with the shared key created in (2).
5. Alice sends to Bob the encrypted message and the encrypted shared key.
6. Bob decrypts the shared key using his private key.
7. Bob decrypts the encrypted message using the shared key.



https://betterprogramming.pub/an-introduction-to-public-key-cryptography-3ea0cf7bf4ba

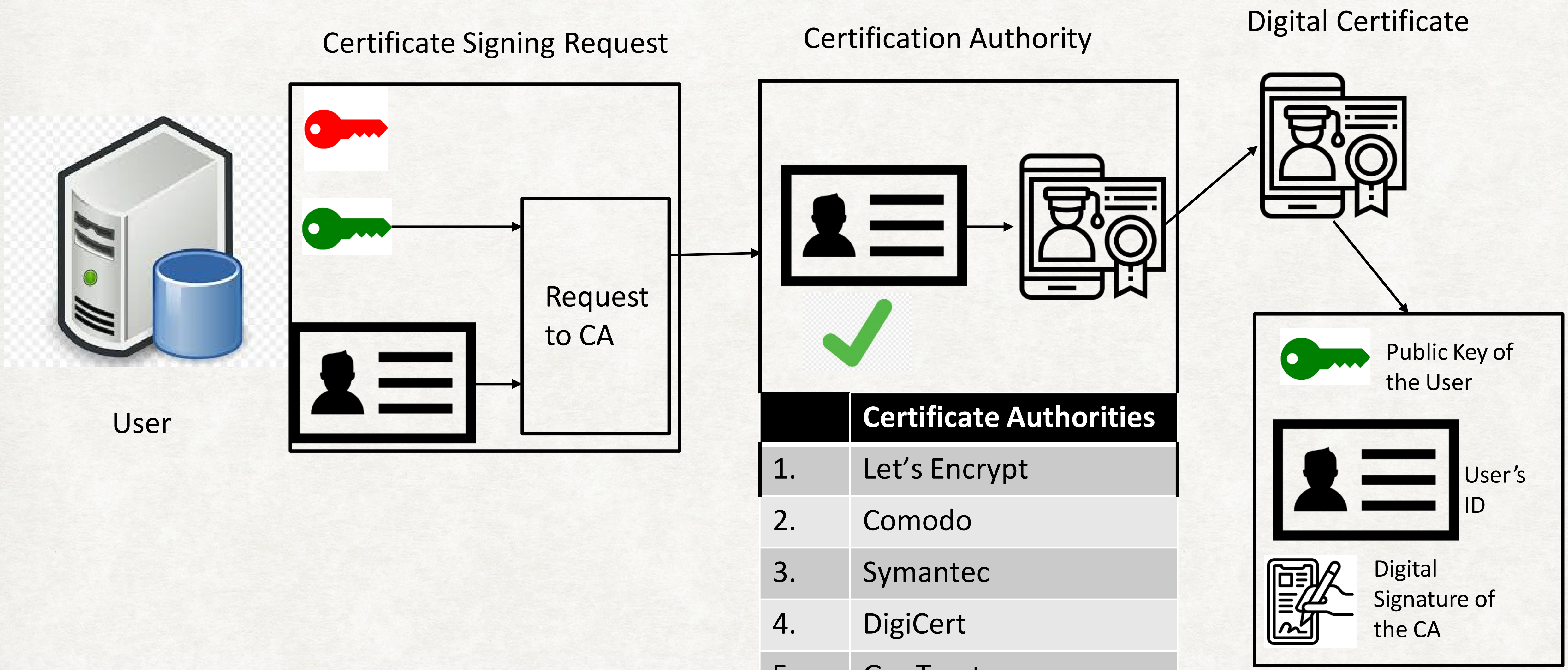
DIGITAL CERTIFICATES

There is still however, one problem in secret key distribution.
How does the client know that the server's public key is actually the **server's** public key, and not some *impostor's* public key?

This is where **digital certificates** come in.

Certificates are issued by well-known *certificate authorities (CAs)*, whose own certificates come pre-installed with most browsers, for example.

DIGITAL CERTIFICATES

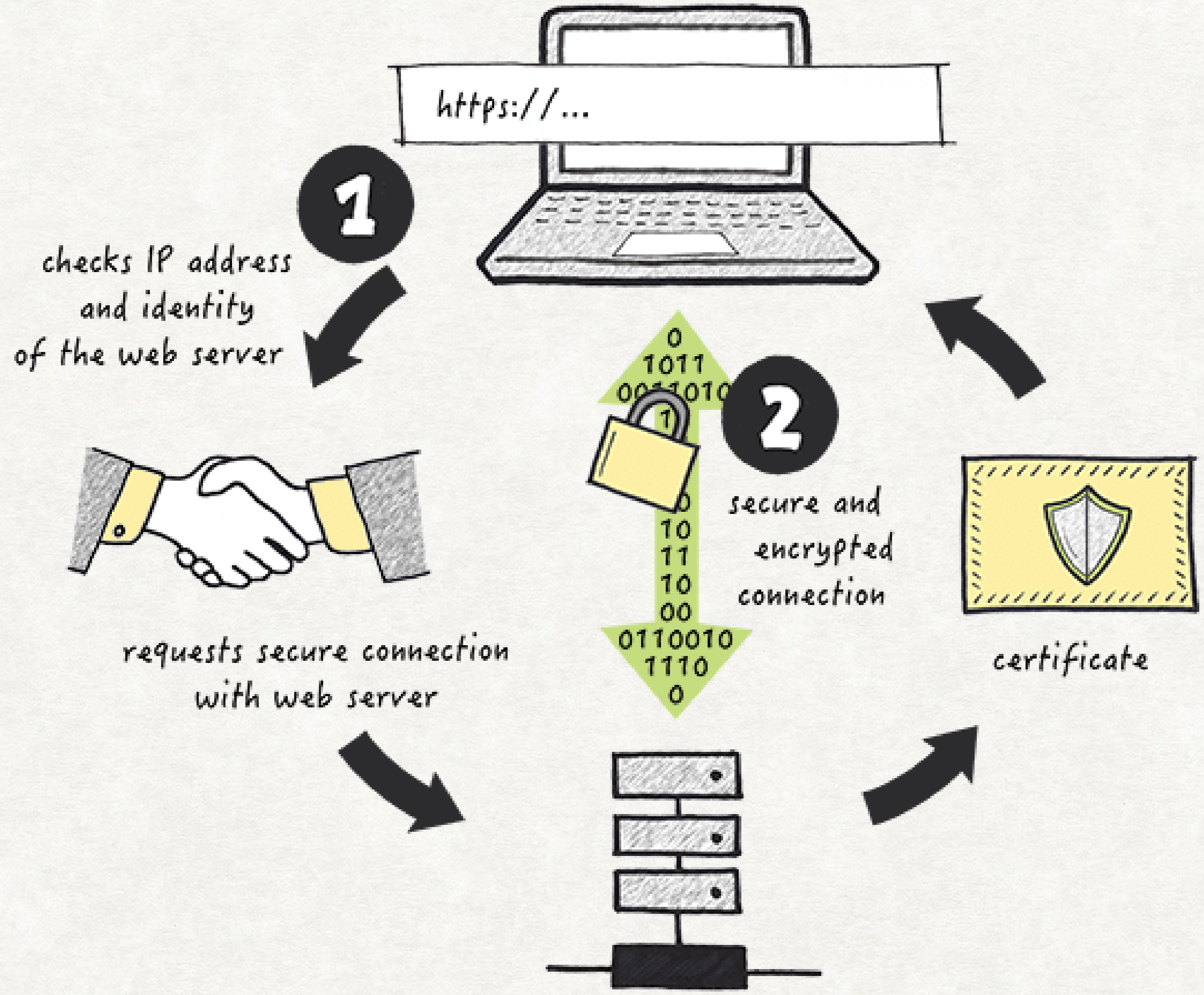


	Certificate Authorities
1.	Let's Encrypt
2.	Comodo
3.	Symantec
4.	DigiCert
5.	GeoTrust

WEB TRANSMISSION SECURITY

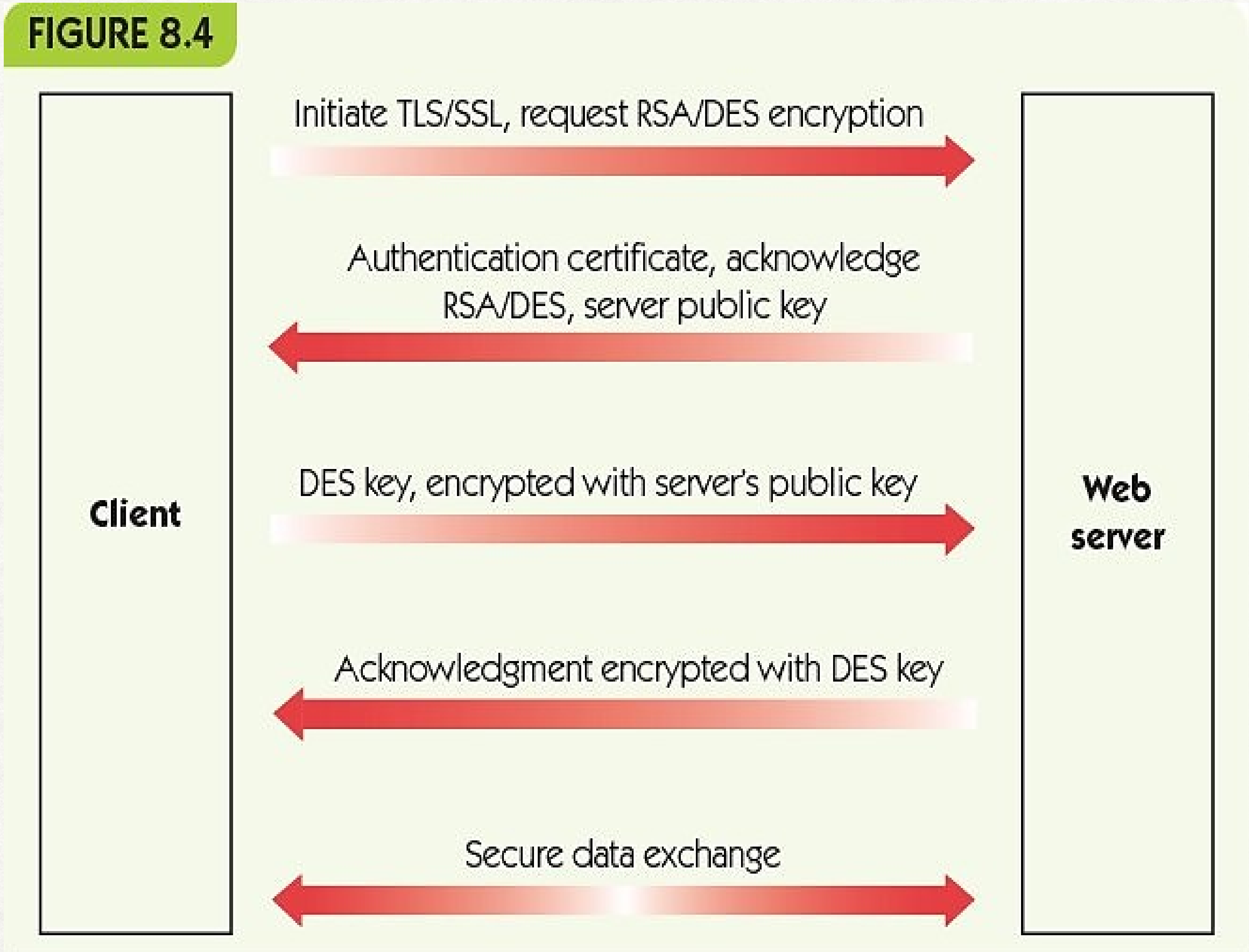
- Ecommerce requires secure transmission of names, passwords, and credit card numbers
- Web protocols: **SSL (Secure Sockets Layer)** and **TLS (Transport Layer Security)**
  - Client-server applications
  - Server provides certificate of authentication (digital certificate) and server’s public key
  - Digital Certificate – issued by trusted third-party certificate authority.
  - Client sends its DES key, encrypted using RSA
  - Data is sent encrypted by the (now shared) DES key

WEB TRANSMISSION SECURITY



The exchange of setup information between the client and the server, preparatory to exchanging real data, is known as a handshake.

WEB TRANSMISSION SECURITY



A typical TLS/SSL session

SUMMARY

- Internet and web are meant to promote information exchange, so information security is hard.
- Online attacks include viruses, worms, Trojan horses, DoS attacks, and phishing, among others.
- Data security involves encrypting sensitive data before transmitting or storing in unsecured location.
- Symmetric encryption requires a shared key.
- Asymmetric encryption uses public and private keys.

Summary

- Caesar cipher is a simple symmetric encryption; substitution ciphers are similar.
- Block ciphers combine blocks of plaintext symbols into blocks of ciphertext.
- Secure web transmission requires protocols: SSL/TLS.